Amendments to the Specification:

Please replace the paragraph extending from page 2, line 12 to page 2, line 22 with the following amended paragraph:

Single-Sign-on (SSO) technology manages this set of multiple identities on behalf of a user so that the user only needs to maintain a single user identity. The user then allows the SSO environment to manage the other identities automatically whenever the user attempts to access a particular protected resource. Some SSO technology stores all of the user's passwords in a centralized database. However, since passwords are confidential, the SSO server uses a "master key" to encrypt the ~~users~~ user's passwords before it stores them and it uses the "master key" to decrypt the user's passwords after it retrieves them from the database and before it sends them to the SSO client.

Please replace the paragraph extending from page 22, line 8, to page 22, line 27 with the following amended paragraph:

Figure 9 depicts a flowchart illustrating a process of determining the password policy in effect for a set of user target passwords and applying the password policy attributes found to a list of user target passwords by generating random passwords in accordance with a preferred embodiment of the present invention. **Figure 9** is a more detailed view of step **706** in **Figure 7**. In this example, the operation begins with a determination as to whether or not a user level change password policy was found (step **902**). If a user level change password policy was found (step **902:YES**), then random passwords are generated ~~suing~~ using the user level password policy (step **904**). Then a determination is made as to whether or not the user level password policy was found for all target passwords (step **906**). If the user level change password policy is not found for all of the target passwords (step **906:NO**), then a determination is made as to whether or not an organizational level change password policy is found (step **910**). If the user level

change password policy was found for all target passwords (step **906:YES**), then the updated list of user target passwords ~~are~~ is passed to the client (step **908**) and thereafter the operation terminates.